CLAIMS

1. A method for carrying out secure signing of a person on a data packet(s) sent from a sender to a recipient, said sender and said recipient connected to a data network via network connection means, comprising the steps of:

a) sampling one or more biometric sample(s) of said person and converting said biometric sample(s) to a digital form;

b) producing a first digital seal from the combination of said digital data packet(s) and said biometric sample(s), or from two or more digital seals derived from said digital data packet(s) and said biometric sample(s);

c) sending said digital data packet(s) and said biometric sample(s) and said digital seal to said recipient;

d) producing a second digital seal from said combinations of received digital data packet(s) and said received biometric sample(s);

e) comparing said first and said second seals; and

f) if said first and said second seals are identical, approving the authentication of said digital signature, otherwise denying the authentication of said digital signature.

2. A method according to claim 1, further comprising:

a) providing a system for sampling biometric samples and storing the same in digital form;

b) providing means for encrypting data at the sender's location;

c) providing means for decrypting data at the recipient's location;

d) sampling one or more biometric sample(s) and converting said biometric sample(s) to digital form;

e) producing a first digital seal from said digital data packet(s) and said biometric sample(s);

f) encrypting said digital data packet(s), said biometric sample(s) and said first digital seal or said two or more digital seals by said encryption means;

g) sending said encrypted data to said recipient;

h) decrypting said encrypted data by said recipient;

i) producing a second digital seal from said received digital data packet(s) and said received biometric sample(s);

j) comparing said first and said second seals; and

k) if said seals have been found identical, approving the authentication of said digital signature, otherwise denying the authentication of said digital signature.

3. A method according to claim 2, wherein said encryption/decryption is carried out by using private and/or public keys.

4. A method according to claim 1 or 2, further comprising the steps of:

a) providing a computerized server for managing the signing process, said server being connected to a network via network connection means;

b) providing a database system for storing signed data packet(s), unsigned data packet(s), a list of authorized users, said users' personal details and biometric templates, said database system accessible by said server;

c) providing one or more client terminal(s) for managing the signing process at the user's location, said terminal(s) being coupled with means for carrying out biometric samples, said terminals(s) being connected to said network via network connection means;

d) providing a list of users authorized for carrying out a digital signature, said users list, said users' personal details and their template(s) being stored in said database system;

e) providing a software component at the client's terminal for producing a template of a biometric sample;

f) providing another software component for comparing digital seals;

g) sending a request for carrying out a digital signature to said server;

At said server's location:

h) upon receiving a request for carrying out a digital signature from a client's terminal, generating a digital ID associated with said session;

i) sending said digital ID from said server to said client terminal;

At said client's location:

j) upon receiving a digital ID from said server, producing a digital package comprised of said digital ID, the personal information and the template and/or the image of a sample of said user;

k) adding a digital seal of said digital package to said digital package;

l) sending said digital package to said server;

m)identifying said user by the personal details comprised in said digital package;

n) authenticating said user's signature by comparing said received template with the template of said user which is stored in said database;

o) producing a second digital seal of said received digital package; and

p) upon positive results in said verification and said authentication and said comparison, approving the authentication of said digital signature, otherwise denying the authentication of said digital signature.

5. A method according to any one of claims 1 to 4, further comprising the steps of:

a) providing means for encrypting and decrypting of data, said means residing on said server and said client(s);

b) encrypting any data to be sent; and

c) decrypting any received data.

6. A method according to claim 4, wherein said digital ID is obtained randomly.

7. A method according to any one of claims 1 to 4, wherein said digital seal is derived from a hash function.

8. A method according to any one of claims 1 to 4, wherein said encryption-decryption is symmetric/asymmetric.

9. A method according to any one of claims 1 to 4, wherein said biometric sample(s) is chosen from fingerprint(s), voice, speech, face, retina, iris, handwritten signature, hand geometry, veins.

10. A method according to any one of claims 1 to 4, wherein said data is sent via the Internet and/or via the Intranet and/or via a WAN (Wide

Area Network) and/or via a LAN (Local Area Network) and/or via a WAP (Wireless Application Protocol) and/or via the telephone network and/or by FTP (File Transfer Protocol) and/or by e-mail.

11. A system for carrying out secure digital signature on one or more digital data packet(s) comprising:

- a computerized server for managing the signing process, said server being connected to a network via network connection means;
- a database system for storing signed data packets, unsigned data packets, a list of authorized users, said users' personal details and biometric templates, said database system accessible by said server;
- one or more client terminal(s) for managing the signing process at the user's location, said terminal(s) being coupled with means for carrying out biometric samples, and connected to said network via network connection means;
- a software component at the client's terminal for producing a template of a biometric sample; and
- a software component for comparing digital seals.

12. A system according to claim 11, further comprising means for encrypting and decrypting of data, said means residing on said server and said client(s) terminal(s).

13. A system according to claim 11, wherein said client's terminal is a computer or a set-top box or a mobile phone.

14. A method for carrying out secure signing of a person on a data packet(s), substantially as described and illustrated.

15. A system for carrying out secure signing of a person on a data packet(s), substantially as described and illustrated.